Northwestern

Exploiting Accelerated Aging Effect for On-line Configurability and Hardware Tracking

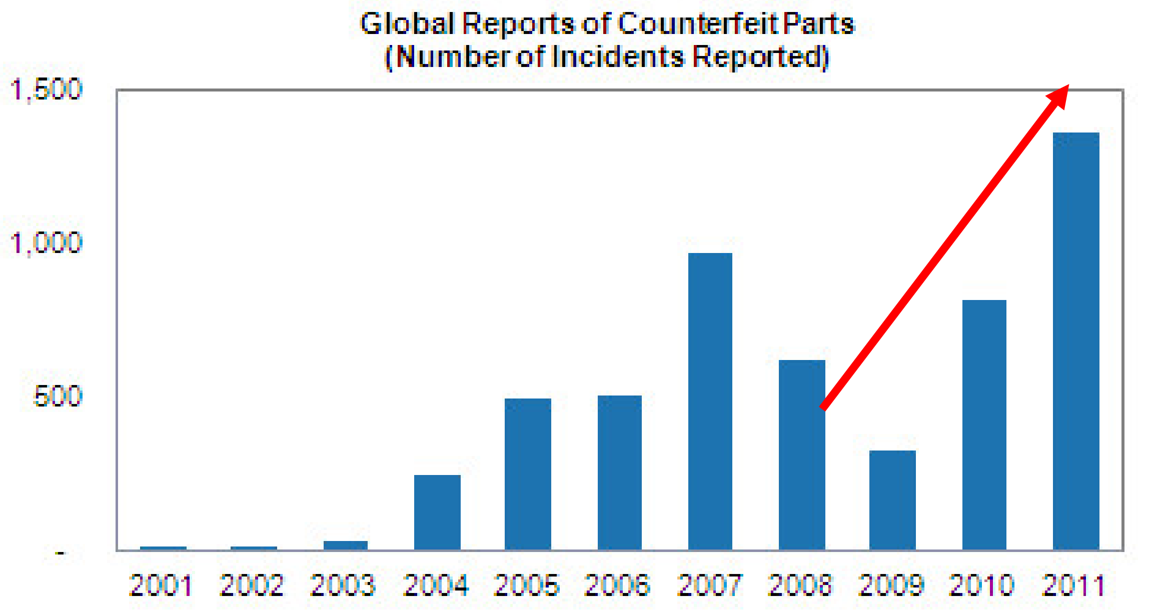
Yang You, Jie Gu

Department of Electrical Engineering and Computer Science (EECS)
Northwestern University
Evanston, IL, USA

Outline

- Introduction
- Aging Model
- Circuit Design of Aging Accelerator
  - System architecture
  - Key challenges and solutions
- Stochastic Processing for Variation Tolerance
- Simulation Results
- Conclusion

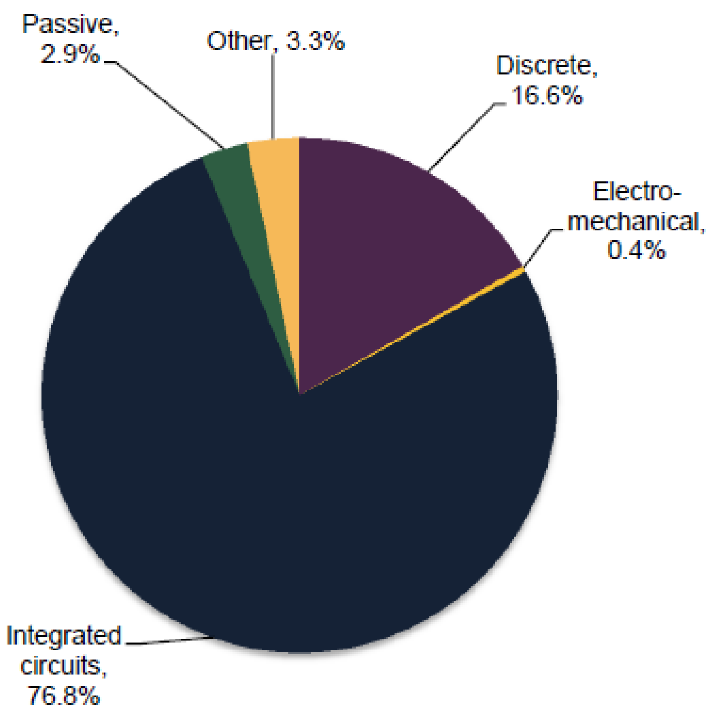
Application of Hardware Tracking

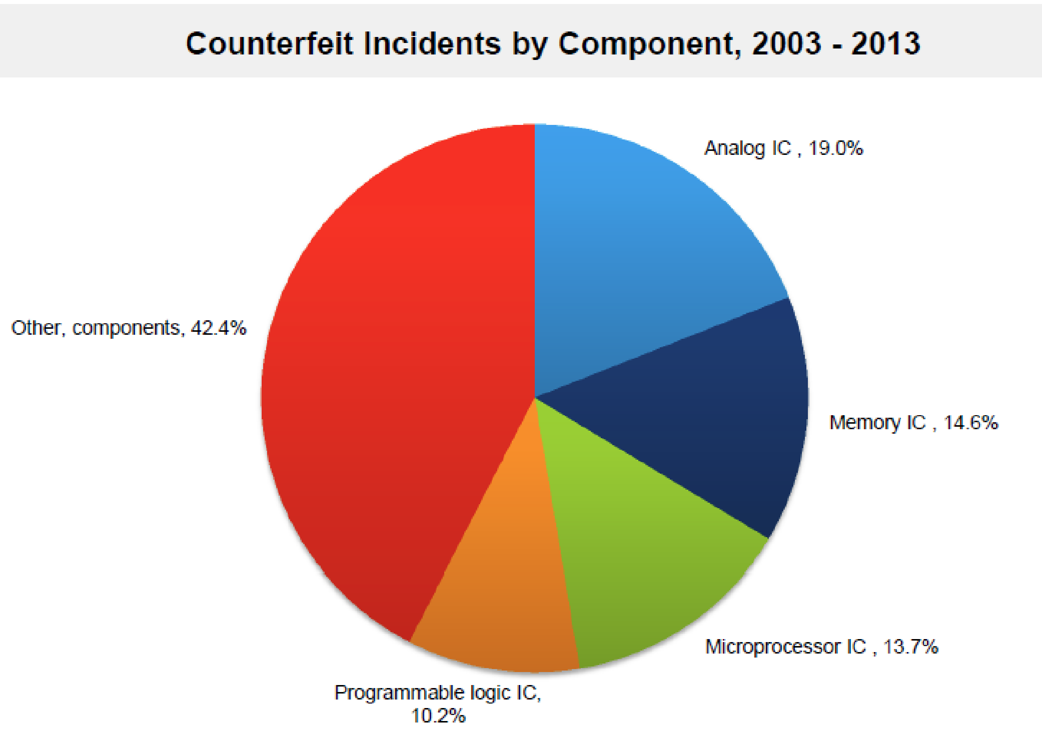


Source: IHS Parts Management
Figures represent ERAI Suspect Counterfeit or High Risk Part Incidents and GIDEP Suspect Counterfeit Alerts for electronic components

- **Detection of Recycled counterfeiting IC**
  - Exponentially rising reports: 8% of merchandise sells
  - Millions of parts annually
  - Severe defense concerns: performance, Trojan injection

Application of Hardware Tracking





HIS Technology, 2014

- **Counterfeiting IC:**
  - 76% of counterfeiting is on IC
  - All IC components observe counterfeiting
  - Analog is the largest victim

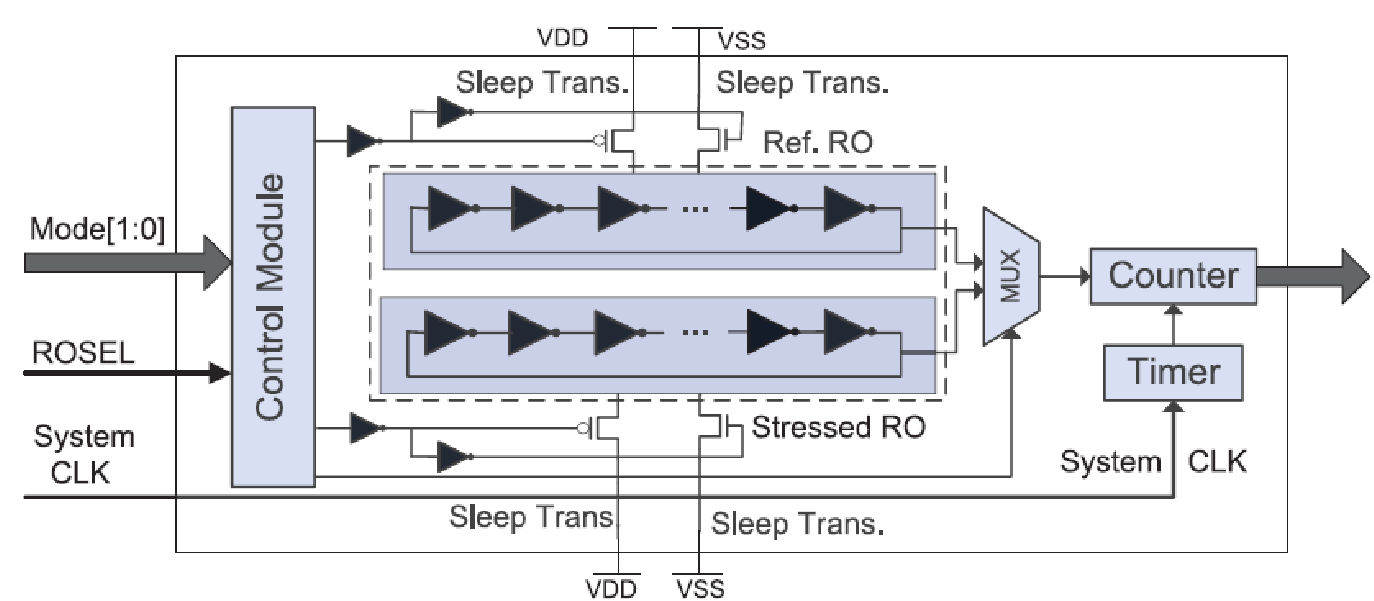
Application of Hardware Tracking

- **Intended termination or degrade functionality after usage**
  - Trial/Demo Chips: limited usage
  - Hardware license key

CMOS Non-volatile Reconfigurability

- Reconfigurability is highly desirable
  - Customization of chips
  - Recovery of defects
  - Recording of ID and activities
- However, standard CMOS is missing reconfigurability
  - Once chip is built, we cannot change.
- Existing solutions:
  - EFUSE: large components, high voltage or high current
  - MRAM/RRAM: still emerging and expensive today
  - Off-chip storage: expensive and unsecure
- Can we create reconfigurability in CMOS using aging effect?
  - Silicon is cheap nowadays !

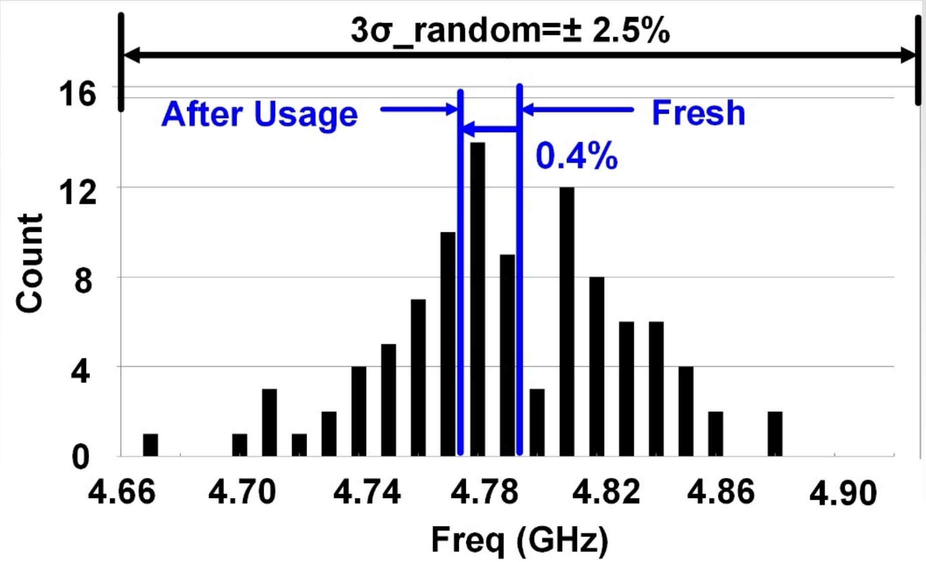
Issues of Previous Aging Sensors



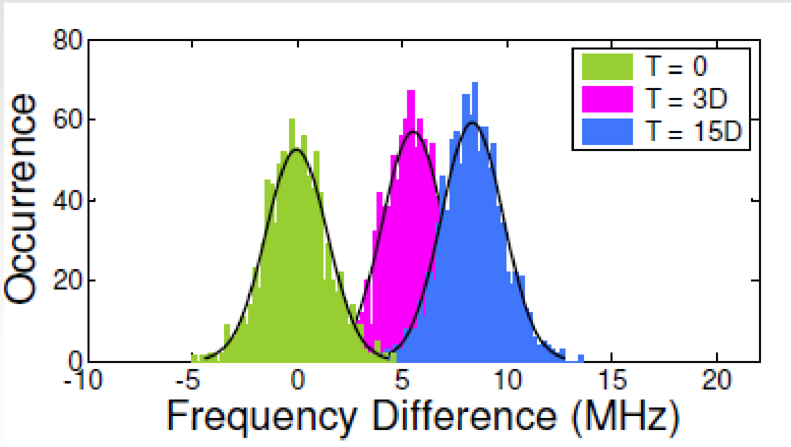
X. Zhang, M. Tehranippor, TVLSI'14

- Significant work has been done on Silicon Odometers
  - Precisely track the usage time of the chips
  - Based on aging effect, such as NBTI
- Alternatively, use Anti-FUSE with large FUSE array to track usage

Issues of Previous Aging Sensors



11 stage RO, 45nm , 10 seconds usage



(f) PV2: 51 Stage RO.

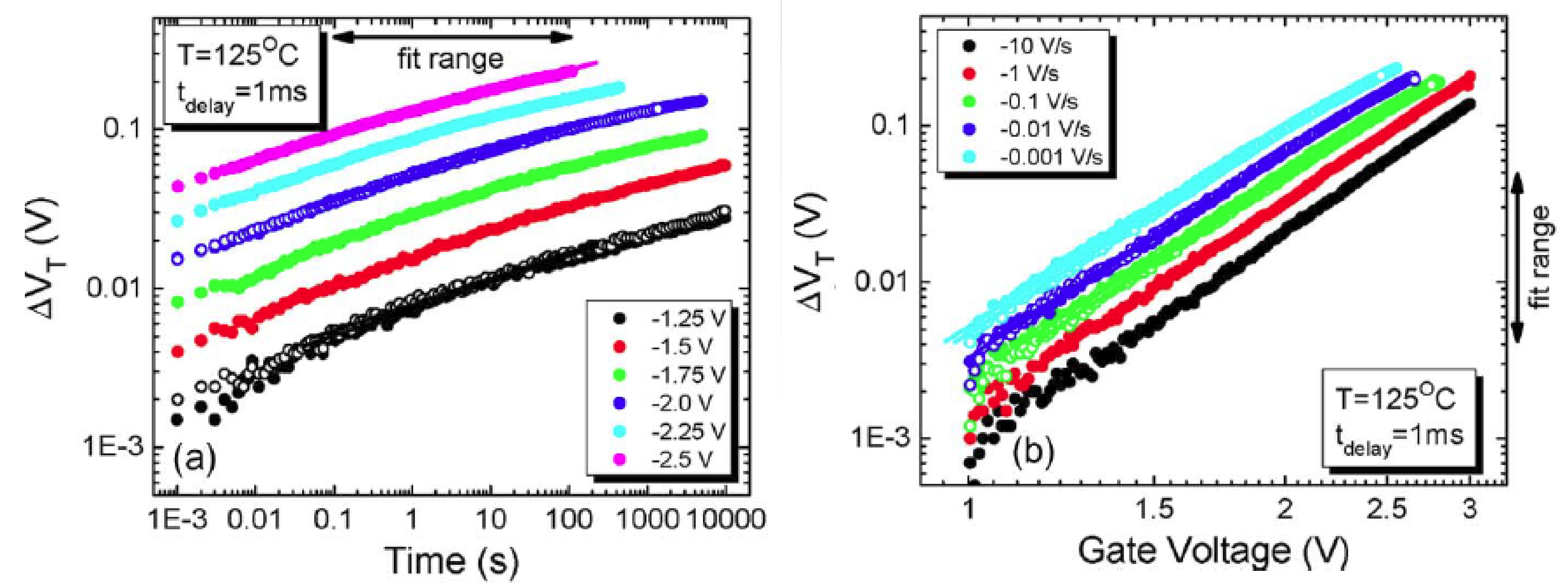
U. Guin, M. Tehranipoor, DAC'14

- Too slow to use natural aging for usage tracking
  - Overwhelmed by random process variation
  - 15 days ~ a few months to reliably detect usage
- Difficulty to detect a fresh chip
  - Report from sensor is random for a fresh chip

Exploiting CMOS Aging Effect

- Our proposed work in this work:
  - **Low cost:**
    - Use CMOS aging effects: NBTI
      - Harder to generate high voltage for TDDB;
      - High power consumption for HCI
  - **Fast tracking:**
    - Minutes of operation
  - **Variation tolerance:**
    - Post-signal processing method to remove variation impact

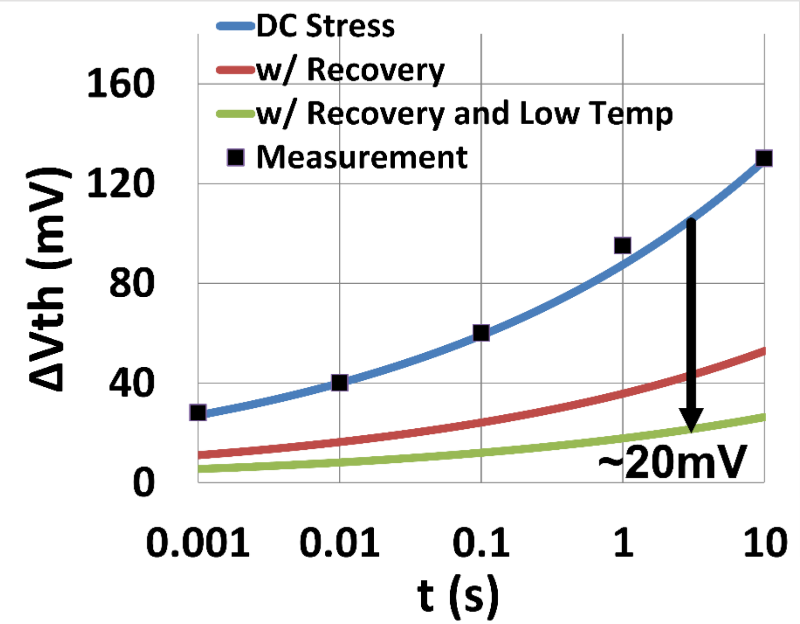
Aging Model used in This work

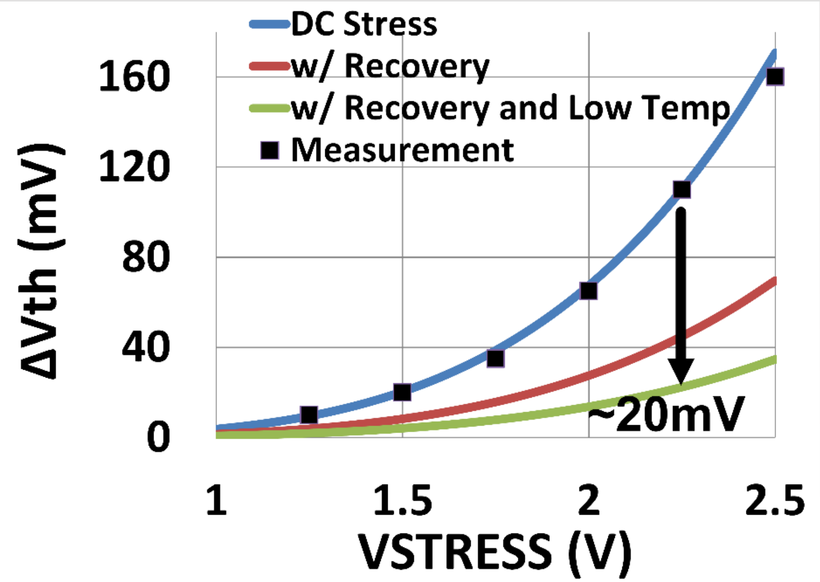


A. Kerber, IEEE Electron Device Letters'09

- Hard to obtain direct model from foundry
- Based on measurement from STM 45nm technology
- Extract ΔVth as a function of Time, Voltage, Temp, Recovery

Aging Model used in This Work



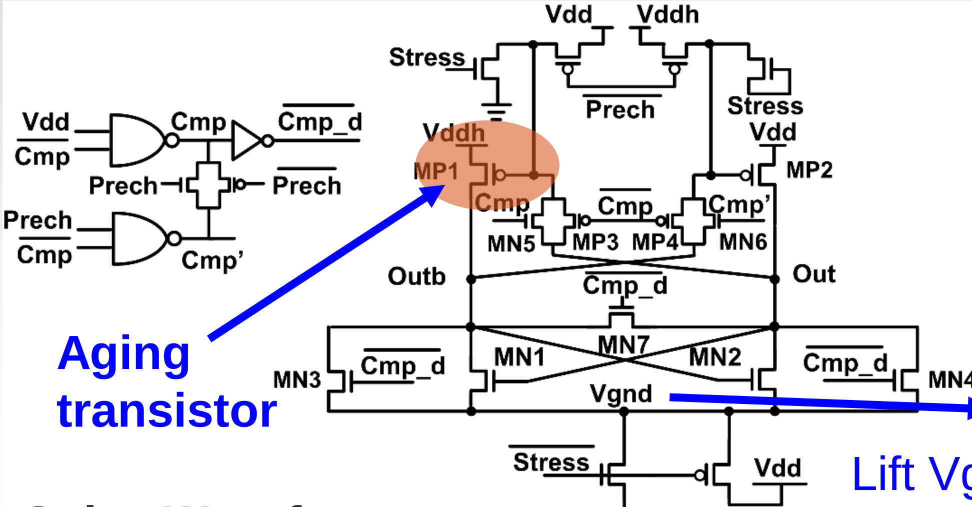


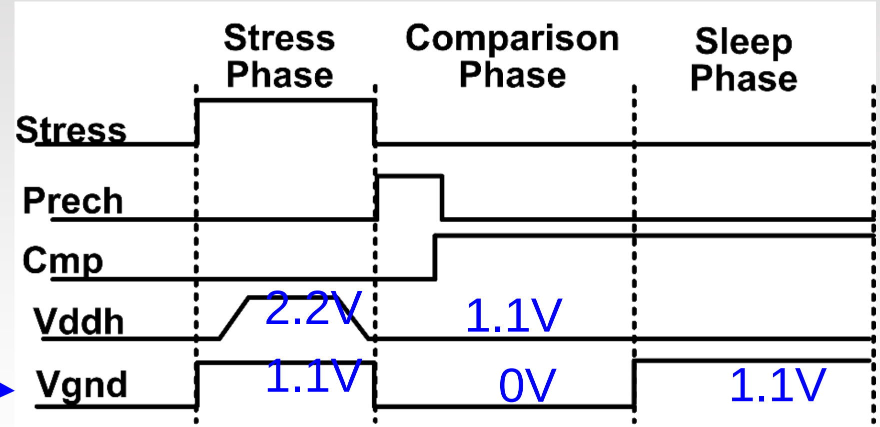
Use widely used Reaction-diffusion model:

$$\Delta V_{th} = A \cdot t^{n} \cdot V_{stress}^{m} \cdot (1 - \eta^{0.5}) \cdot e^{\left(-\frac{nE_a}{kT}\right)}$$

- Curve fitting with Reaction-diffusion model
- Consider worst-case condition: least drift, low temp & recovery
- Example: $\Delta V_{th} = 20mV$ at 2.2V and 2 Second stress

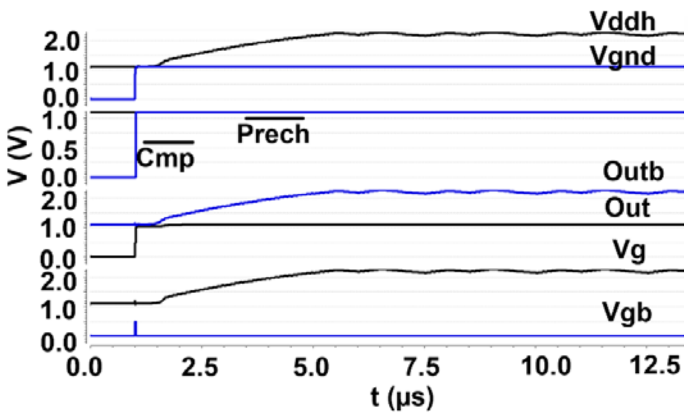
Latch based Aging Accelerator Circuit

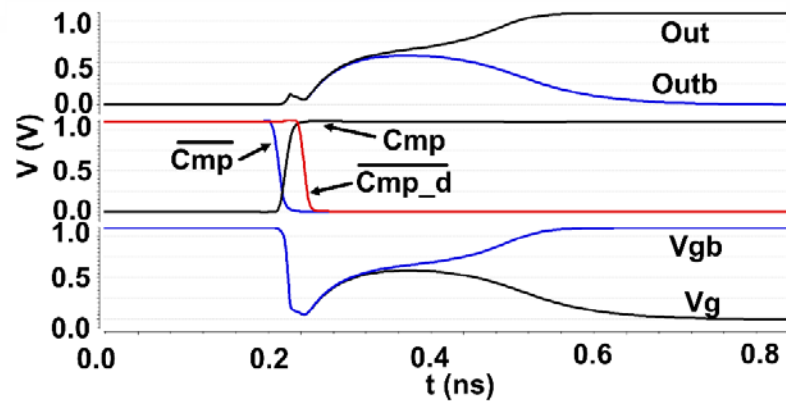




Lift Vgnd to 1.1V to avoid stress

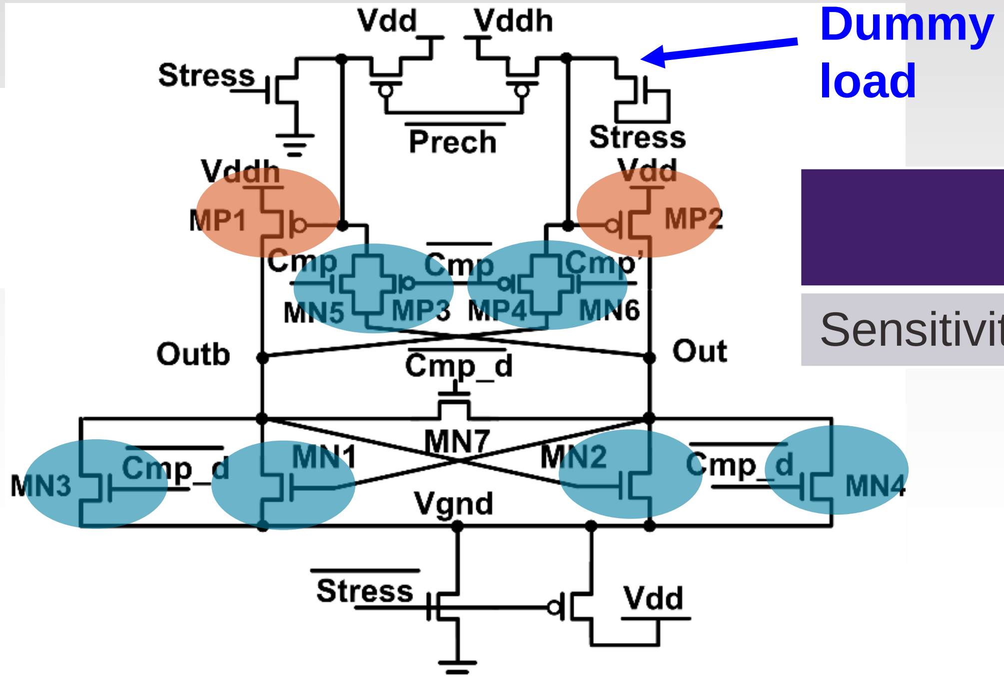
Spice Waveforms:





- Key challenge: at 2.2V at input, no overstress (>1.1V) is created
- Internal nodes are fully symmetrical; No aging in sleep mode

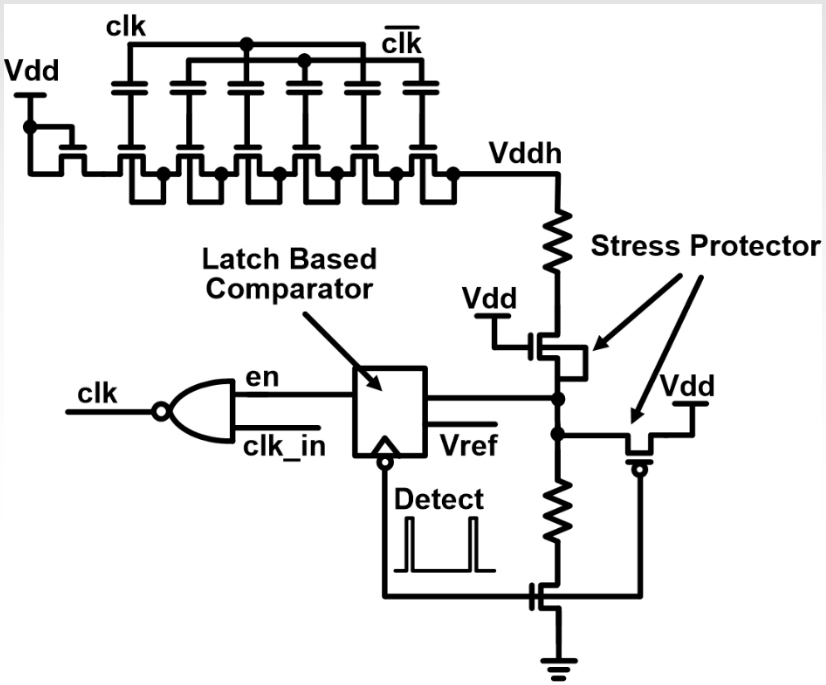
Latch based Aging Accelerator Circuit

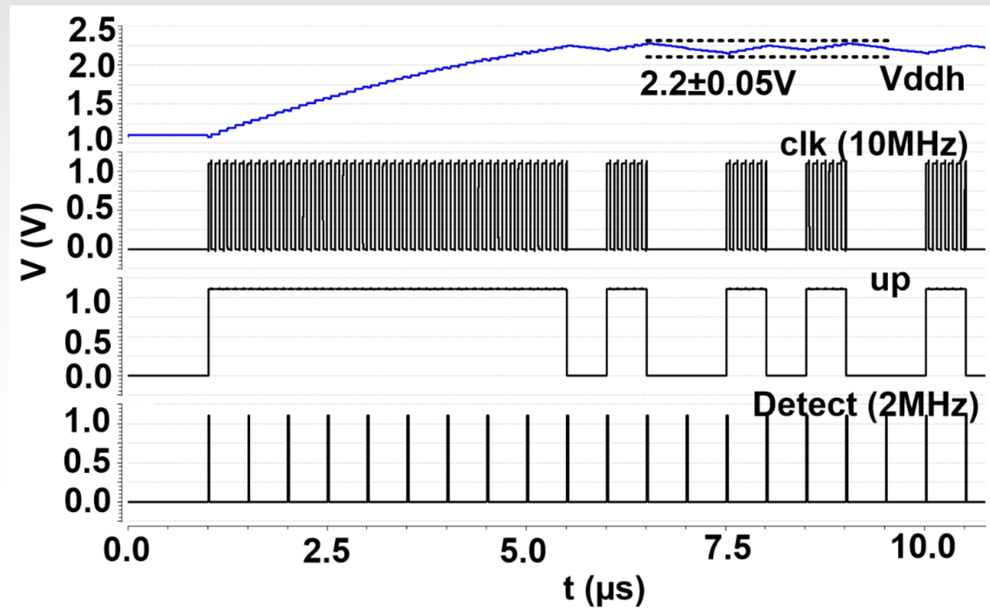


	MP1& MP2	MN1& MN2	MN3&MN4	MN5&MN6&MP3&MP4
Sensitivity	1	0.11	0.1	0.03

- Variation Consideration
  - Output should be determined by mismatch of PMOS transistors
  - Minimizing impacts from remaining transistors
  - Properly sized transistors for improving sensitivity

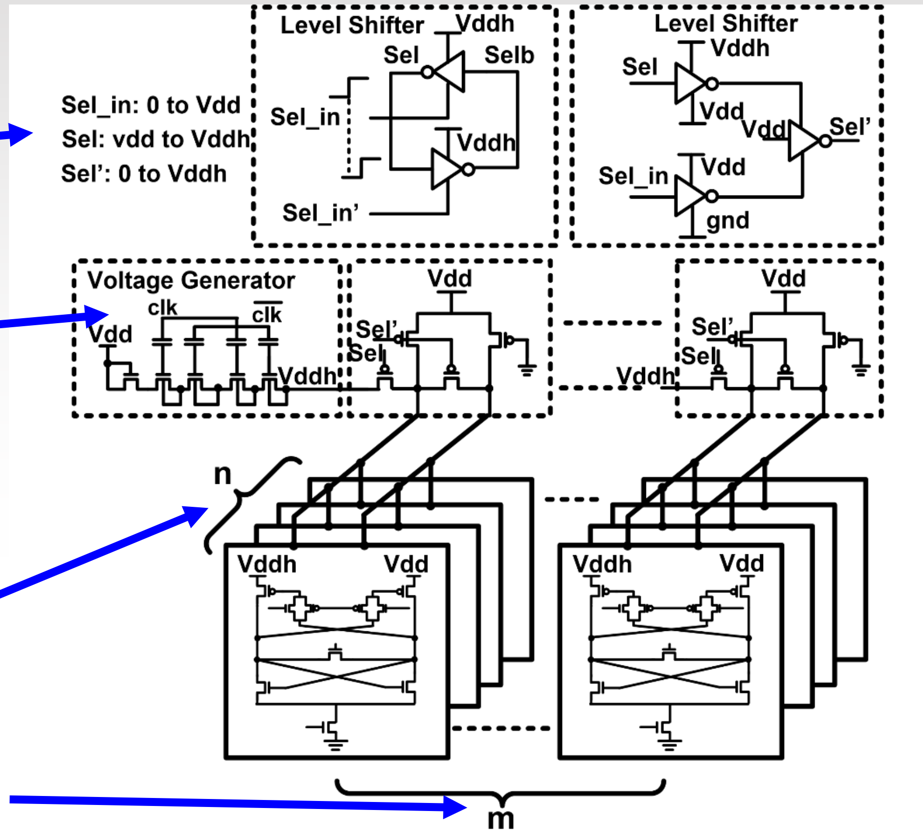
System Design for Aging Accelerator





- Charge pump is designed to generate higher voltage from internal VDD with feedback control
- 10MHz clock and ultra-low power consumption (<10uA)

System Design for Aging Accelerator



Level shifters for digital control

Shared charge pump

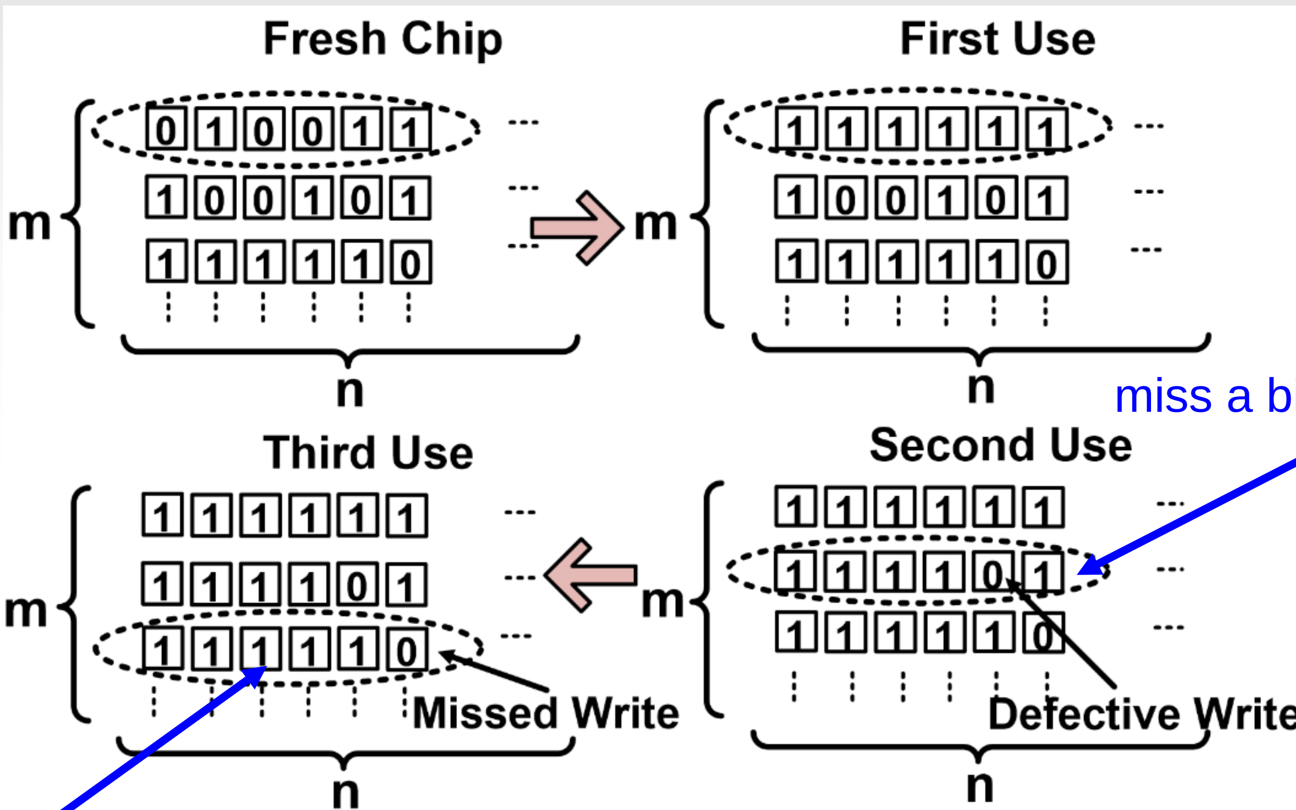
n cells for single usage

m arrays for m times of usage

- ΔV_{th} of ~20mV is not enough to overcome mismatch of devices
- An arrays of devices "n" are used to improve confidence
- For tracking "m" times of usage, "m" arrays are used

System Write Sequence

11111111 ⟹ 11101111 Still consider to be written?



miss a bit due to variation

Incidentally match a write pattern

- **Questions: how many flipped bits can we tolerate?**

Stochastic Analysis for Variation Tolerance

Assume we can tolerate "t" flipped bits ("0") for stressed chip

Defective Rate: Stressed chip with failed write

$$DR(s) = p^s \cdot (1-p)^{n-s} C(n,s)$$

$$= p^s \cdot (1-p)^{n-s} \cdot \frac{n \cdot (n-1) \cdot (n-2) \dots (n-s)}{s! \cdot 2^n}$$

$$DR_{all} = \sum_{s=t+1}^{\infty} DR(s) = \sum_{s=t+1}^{\infty} p^s (1-p)^{n-s} C(n,s)$$

($p = f(\Delta V_{th})$ is the probability of single cell being flipped)

t

10101100 $\xrightarrow{\text{after write}}$ 11101011

Miss Rate: Unstressed chip with incidentally stressed pattern

$$MR(s) = \frac{C(n,s)}{2^n} = \frac{n \cdot (n-1) \cdot (n-2) \dots (n-s)}{s! \cdot 2^n}$$

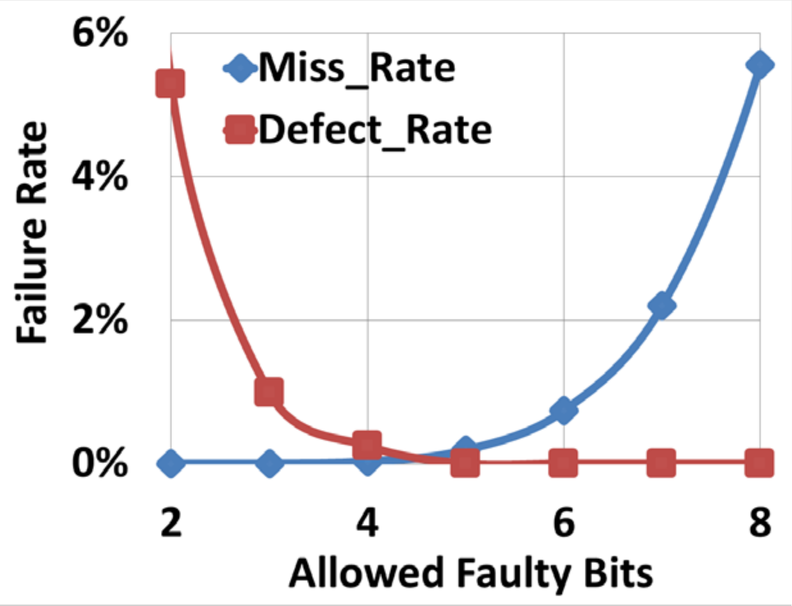
$$MR_{all} = \sum_{s=0}^{t} MR(s) = \sum_{s=0}^{t} C(n,s)/2^n$$

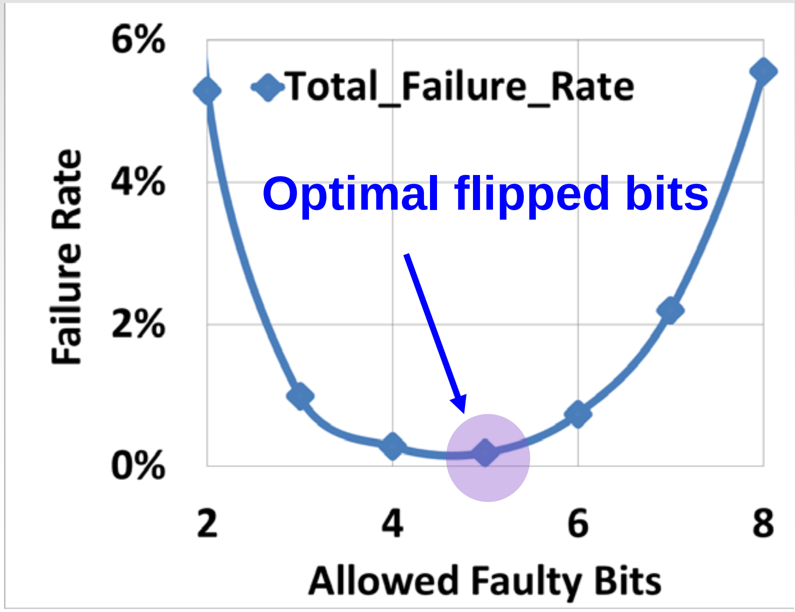
11101011 $\Rightarrow$ no write

Total Failure Rate: (to be minimized)

$$FR = MR_{all} + DR_{all} = \sum_{s=0}^{t} C(n,s)/2^n + \sum_{s=t+1}^{\infty} p^s (1-p)^{n-s} C(n,s)$$

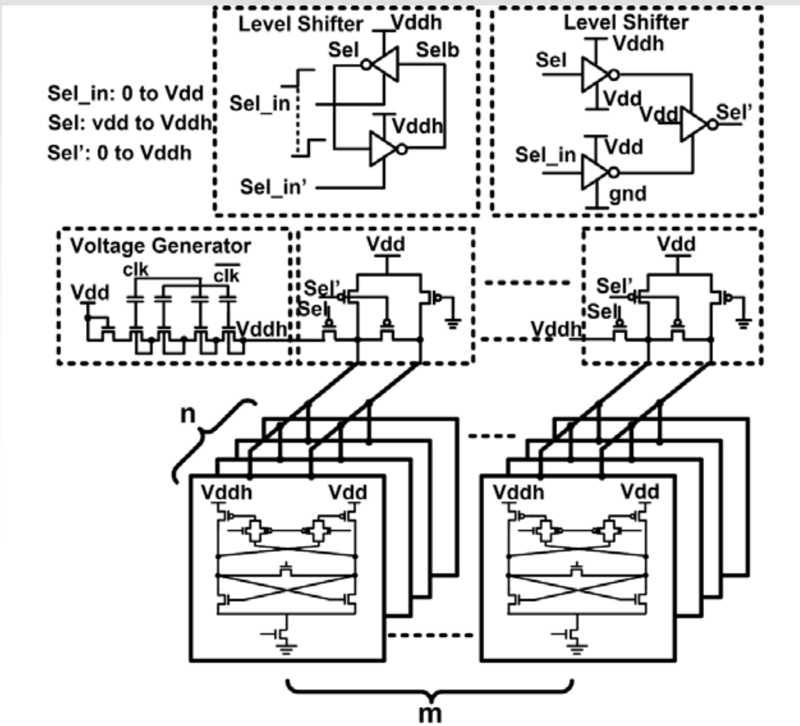
Stochastic Analysis for Variation Tolerance



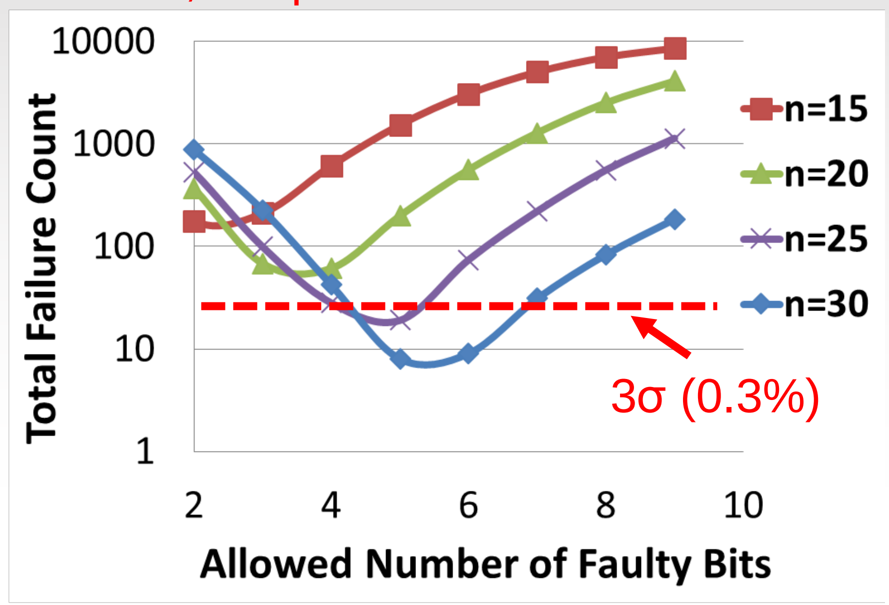


- Tradeoff between miss rate and defect rate
- Optimal # of allowed flipped bits can be found

Design Optimization for Variation Tolerance

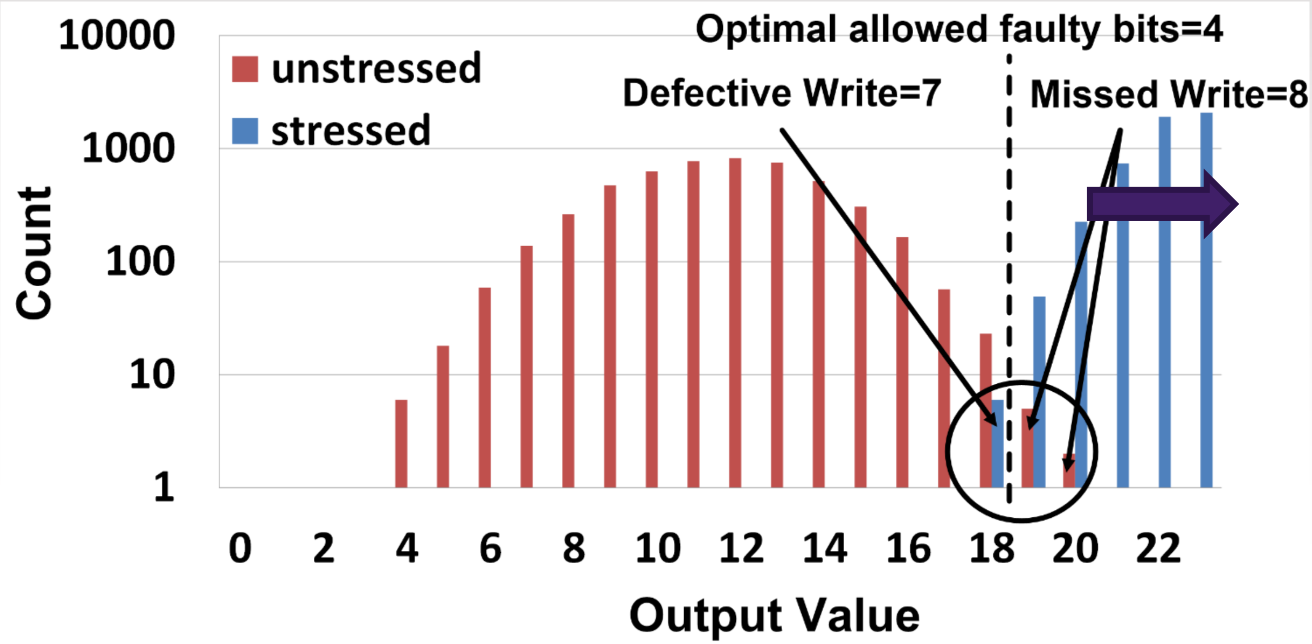


10,000 points Monte-Carlo simulation



- Determine number of cells (n) to reach target failure rate
- For 3σ tolerence, ~22 cells are needed

Transistor Level Simulation Verification

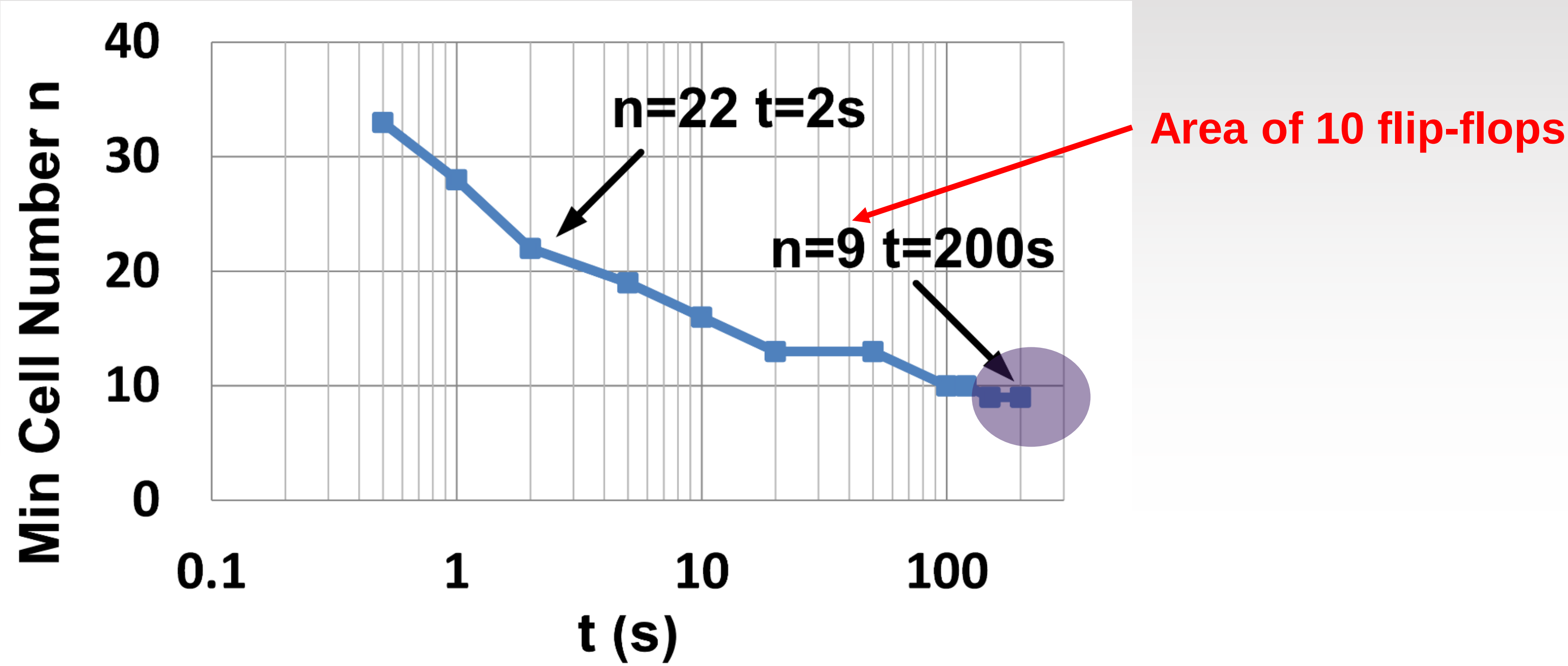


Item	Value
Technology	45nm
Cell size	11µm^2
Power	25µW

Compatible with standard flip-flop

- Use full-transistor schematics
- Performed 5,000 Monte-Carlo simulation in 45nm CMOS at 1.1V
- After stress, most cells move to target output >=18
  - 7 defective write and 8 missed write > 0.3% failure rate
- Matches analysis and equations
- n=23 > 22(predicted) mostly due to variation from other components

Stress Time versus Cell Count



- Only 9 cells needed for 3 minutes; But 22 cells for 2 second
- It is possible to finish tracking within seconds to minutes time
- A tradeoff between hardware cost and test time

Conclusions

- An CMOS accelerator based aging effect is built for tracking usage
- Latch based design
  - Low cost => compatible with standard flip-flop
  - No overstress on supporting devices
  - Simple system configuration
- Fast tracking through proposed schemes:
  - Accelerated aging with high voltage
  - System level stochastic processing
- Verification with Monte-Carlo simulation in 45nm CMOS
  - Up to 2 seconds stress time
  - 25µW power consumption

Thank you!

Department of EECS

Northwestern | McCORMICK SCHOOL OF ENGINEERING